REMARKS

Applicants appreciate the thorough examination of the present application that is reflected in the Official Action of July 30, 2004. Applicants also appreciate the Examiner's citation of U.S. Patent 6,125, 192 to Bjorn et al. ("Bjorn"), U.S. Patent No. 5,229,764 to Matchett et al. ("Matchett"), and U.S. Patent No. 6,325,285 to Baratelli. Applicants have canceled Claims 1-25, 28-59, 62-93, and 96-102 to expedite prosecution. Applicants have now carefully studied Bjorn, Matchett, and Baratelli, and respectfully submit that the remaining pending Claims 26, 27, 60, 61, 94, 95, and 103-105 are patentable over these references for the reasons that now will be described.

The "Related Inventions" Section has Been Amended

In response to the objection to the "Related Inventions" section on page 1 of the specification, Applicants have amended the section to provide the corresponding issued U.S. patent numbers and serial number where available. Accordingly, Applicants respectfully submit that the objection relating thereto has been overcome.

The "Abstract" Section has Been Amended

In response to the objection to the "Abstract" section of the specification, Applicants have amended the Abstract to remove the recitation of "the disclosed techniques". Accordingly, Applicants respectfully submit that the objection relating thereto has been overcome.

The Hyperlinks Have Been Removed and Trademarks Usage Has Been Amended

In response to the objection to the specification of page 4, line 16 and page 29, line 7, the hyperlinks have been changed by removing "http:\\" from the hyperlinks, so that there no longer are executable hyperlinks in the specification. Accordingly, Applicants respectfully submit that the objections relating thereto have been overcome.

Moreover, the specification has been reviewed and amended for proper usage of trademarks as appropriate. Accordingly, Applicants respectfully submit that the objections relating thereto have been overcome.

Claim Amendments

Claims 60, 61, and 103-105 have been amended to eliminate recitations of "step". Claims 94 and 95 have been amended to eliminate "means" language in these computer program product claims. Claims 26-27, 60-61, 94-95, and 105 have also been amended to correct informalities as will now be described.

Objection of Claim 105 has Been Overcome

Claim 105 has been amended to remove the recitation of "aborting the security-sensitive operation". Accordingly, Applicants submit that the objection to Claim 105 has been overcome.

Rejections of Claims 26-27, 60-61, and 94-95 Have Been Overcome

Claims 26-27, 60-61, and 94-95 have been amended to recite "a security core". Accordingly, Applicants submit that the rejections under 35 USC §112, second paragraph, have been overcome.

Applicants File Herewith a Terminal Disclaimer to Overcome the Provisional Obviousness-Type Double Patenting Rejection of Claims 103-105:

Claims 103-105 have been provisionally rejected under a nonstatutory judicially created doctrine of obviousness-type double patenting over copending U.S. Application Serial No. 09/764,844 in view of U.S. Patent No. 5,229,764 to Matchett et al. Applicants submit herewith a Terminal Disclaimer disclaiming additional term over the copending U.S. Application Serial No. 09/764,844. Applicant's agreement to provide a Terminal Disclaimer is to expedite issuance of the present case and does not admit that the present invention is obvious in light of the copending U.S. Application Serial No. 09/764,844 or Matchett. Withdrawal of the obviousness-type double patenting rejection is respectfully requested.

Independent Claims 26, 27, 60, 61, 94, 95, and 103-105 Are Patentable Over Bjorn in view of Matchett.

Independent Claims 26, 27, 60, 61, 94, 95, and 103-105 have each been amended to independent form, and contain analogous recitations.

Amended independent Claim 26 stands rejected under 35 USC §103(a) over Bjorn in view of Matchett. Claim 26 recites:

> 26. A system for providing continuous authentication of a user of a computing device, comprising:
> a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;
> a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;
> securely-stored biometric information which identifies an owner of the computing device;
> means for repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device, wherein the means for repeatedly obtaining is activated upon beginning a security-sensitive operation and is terminated upon completion of the security-sensitive operation;
> means for comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user; and
> means for concluding, within a security core, that the security-sensitive operation is authentic based on all other components which are securely operably connected to the security core remaining securely operably connected until completion of the security-sensitive operation.

Accordingly, the system includes a security component that provides security functions that can vouch for authenticity of components with which it is securely operably connected. Biometric input of a user is repeatedly obtained from a biometric sensor component during a security-sensitive operation. Within a security core, the security-sensitive operation is determined to be authentic so long as the other components (the components other than the biometric sensor that are to be authenticated) remain securely operably connected to the security core during the security-sensitive operation.

The specification of the present application describes the security core, and authentication of components attached thereto, in accordance with some embodiments of the present invention, as follows:

> In the preferred embodiments, components that authenticate themselves to the security core must remain physically attached thereto throughout an application function. Application-specific processing may be provided within each application processing subsystem to handle detachment of a component. For example, if camera module 130 is unplugged from the security core in the middle of taking a photo, the camera would have no way to transmit the photo (since it is preferably dependent on the security core for power, I/O, image storing, and so forth). If this module 130 is subsequently plugged in to a second (different) security core, that second security

> core would preferably stamp any pre-existing data in the camera as "unsecure" as the data traverses the second core (for example, on its way to the I/O bus of the second integrated device for purposes of storing captured images in persistent storage). (Alternatively, the second device may be adapted such that it will not accept any previously-created data.) Marking a data stream "unsecure" indicates the security core's inability to vouch for the authenticity and untampered state of I/O or application processor data.

(Specification, Page 21, line 18 - Page 22, line 11.)

Accordingly, the security core may conclude that a security sensitive operation with a component is not authentic if that component is disconnected, and may treat data that is later received from the reconnected component as "unsecure".

The Office Action appears to concede that Bjorn does not disclose at least the "means for concluding" as recited in Claim 26. However, the Office Action cites to Matchett in an attempt to provide the missing teaching.

Applicants note that the Court of Appeals for the Federal Circuit has affirmed that to support combining or modifying references in a § 103 rejection, evidence of a suggestion, teaching, or motivation to combine or modify must be *clear and particular*, and this requirement is not met by merely offering broad, conclusory statements about teachings of references. *In re Dembiczak*, 50 USPQ2.d 1614, 1617 (Fed. Cir. 1999). In an even more recent decision, the Court of Appeals for the Federal Circuit has stated that, to support combining or modifying references, there must be particular evidence from the prior art as to the reason the skilled artisan, with no knowledge of the claimed invention, *would have selected these components for combination in the manner claimed*. *In re Kotzab*, 55, USPQ2d 1313, 1317 (Fed. Cir. 2000).

The Office Action on Page 11 states that "Matchett et al. discloses the limitation of wherein the means for concluding ..., for example (see column 10, lines 2-10)." Applicants respectfully submit that the Office Action has not provided evidence of a suggestion, teaching, or motivation, and much less, has not provided *clear and particular* evidence to combine or modify Bjorn to include the teaching of Matchett to disclose the recitations of Claim 26.

However, for the sake of argument, even if Bjorn is combined with Matchett, they still would not teach the "means for concluding" as recited in Claim 26. The Office Action cites to Matchett, Col. 10, lines 2-10, which teaches the following:

> Security protection could be enhanced by instructing the protected system to shut down should it be disconnected from the system 400 according to the present

invention. Using such connection-dependent instructions, the protected computer's keyboard could be connected through a chassis of the system 400 according to the present invention.
(Matchett, Col. 10, lines 2-10).

Accordingly, Matchett teaches that a protected device itself can shut down if it is disconnected from the security system. With reference to FIG. 1 of Matchett, a protected device (shown as "protected device control") can shut itself down if it is disconnected from the authentication system 100. However, Matches does not suggest that the authentication system 100 makes any determination of authenticity of a security-sensitive operation based on the protected device becoming disconnected. Accordingly, if the protected device is reconnected to the authentication system 100, the data that is subsequently received would not be treated differently than if the protected device had not become disconnected.

Furthermore, Matchett does not teach or suggest a security core that can determine the authenticity of a security-sensitive operation based on components (other than a biometric sensor) remaining securely operably connected to the security core during the security-sensitive operation, as recited in Claim 26. Matchett lacks such teaching because it discloses, and is concerned with, protecting only a single protected device. With reference to FIG. 1 of the present application, the security core of the present may protect a plurality of various different types of devices 112-136.

Consequently, Applicants respectively submit that the Office Action has not established a *prima facie* case of obviousness. Accordingly, Applicants request withdrawal of the rejection of Claim 26.
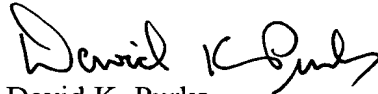
Independent Claims 27, 60, 61, 94, 95, and 103-105 contain analogous recitations to Claim 26, and are respectfully submitted to be patentable over Bjorn in view of Matchett for at least the reasons provided above.

CONCLUSION

In light of the above amendments and remarks, Applicants respectfully submit that the above-entitled application is now in condition for allowance. Favorable reconsideration of this application, as amended, is respectfully requested.

Respectfully submitted,

David K. Purks
Registration No. 40,133

USPTO Customer No. 46589
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401